

ABSTRACT

The present invention provides a system and method for traffic analysis. Embodiments can be used to detect malevolent network activity such as worms, viruses, denial of service attacks, and unauthorized network routing. Upon detecting the activity, steps can then be taken to halt the spread and/or remove the malevolent network activity, thereby adding protection from such activity to the network. Other network activity of interest can also be detected.